BAB I

PENDAHULUAN

1.1 Latar Belakang

Konsep dari *quantum computing* telah menginspirasi banyak sekali ilmuwan, fisikawan, dan ilmuwan komputer. Perkembangan bidang *quantum computing* dapat dilihat dari beberapa demonstrasi eksperimen dalam jangka waktu dua dekade terakhir (C´orcoles, dkk., 2019). *Quantum information processing* adalah bidang yang mencakup *quantum computation, quantum cryptography*, *quantum communications,* dan *quantum games*, bidang ini membawa ide untuk menggunakan mekanika kuantum lebih dari mekanika klasik untuk memodelkan pemrosesan informasi. Teori *Quantum computing* bukan tentang mengubah substrat fisik di mana perhitungan dilakukan dari klasik ke kuantum, melainkan mengubah gagasan tentang komputasi itu sendiri. Perubahan ini terlihat dari pergantian unit dasar perhitungan pada komputer yaitu *bit*, yang diganti menjadi kuantum *bit* atau *qubit* (Rieffel, dkk., 2011).

Komputer kuantum dapat mengungguli algoritma klasik. Hal ini telah lama diakui oleh Richard Feynman seorang fisikawan paling berpengaruh pada abad kedua puluh yang mengatakannya pada tahun 1980-an bahwa masalah mekanika kuantum lebih baik diselesaikan dengan mesin kuantum. Hanya pada tahun 1994 seorang profesor matematika terapan bernama Peter Shor membuat sebuah algoritma yang dapat melakukan pemfaktoran terhadap bilangan prima yang besar lebih cepat dan efisien dibanding dengan komputer klasik (Monz, dkk., 2015).

Hal ini memicu perkembangan penelitian dalam bidang komputasi kuantum (T. Monz, dkk., 2015). Algoritma quantum Shor's Algorithm telah membawa banyak perhatian ke dalam bidang cryptography. Algoritma kuantum Shor's Algorithm adalah algoritma yang berfungsi untuk menyelesaikan Prime Factorization Problem dalam Polynomial Time. Shor's Algorithm mempunyai performa yang lebih bagus dari algoritma General Number Sieve (Lomonaco, 2000).

Sistem kriptografi RSA adalah sebuah *Public Key Algorithm* yang terkenal dibuat oleh Ron Rivest, Adi shamir, dan Len Adleman dan pertama kali dipublikasikan pada tahun 1977. RSA biasanya dipakai untuk menjaga privasi dan autentikasi data digital (Kalpana, 2012). RSA terdiri dari dua proses dasar dalam bidang kriptografi. Pertama adalah penggunaan *public key* untuk mengubah sebuah *plain text* menjadi *cipher text*, sehingga tidak dapat diubah kembali ke bentuk semula tanpa menggunakan tenaga komputasi yang besar proses ini biasanya disebut dengan proses enkripsi. Kedua adalah penggunaan *private key* unttuk mengubah kembali *cipher text* mencadi *plain text* yang dapat dibaca proses ini biasanya disebut dengan proses dekripsi. RSA dipakai dalam *web browser*, *email*, *mobile phone communication*, *virtual private network*, dan *secure shells* untuk menjaga keamanan data (Kota dan Aissi, 2002).

Keamanan dari protokol komunikasi menggunakan RSA *public key encryption system* bergantung kepada usaha komputasi yang besar untuk mencari bilangan faktor prima dari sebuah angka yang besar menggunakan komputer klasik, namun pada tahun 1994, Peter W. Shor menunjukkan bahwa sebuah komputer

kuantum dapat melakukan hal tersebut dengan mudah (Gerjuoy, 2004).

Perkembangan pesat di bidang *quantum computing*, telah menyebabkan muncul beberapa kekhawatiran terhadap penggunaan RSA. Hal ini dikarenakan potensi algoritma *Shor's Algorithm* dalam melakukan pemfaktoran bilangan prima dengan cepat, yang dapat meretas *private* dan *public key* yang mendasari RSA. Jadi jika sebuah komputer kuantum berskala besar dibuat, hal ini dapat membuat banyak *public-key cryptosystem* yang menjadi standar komunikasi menjadi tidak aman (Chen, 2016).

Sebuah algoritma kuantum hanya dapat dijalankan dengan baik pada komputer kuantum, namun komputer kuantum tidak dapat diakses dengan mudah, hanya terdapat beberapa perusahaan yang berpacu dalam bidang kuantum mempunyai akses ke komputer kuantum tersebut. Qiskit adalah sebuah *open-source framewor*k untuk *quantum computing*. Qiskit bertujuan untuk membuat dan memanipulasi *quantum programs* dan menyimulasikan program tersebut ke dalam *prototype quantum device* yang dimiliki IBM Q yang dapat dijalankan dari komputer lokal (Qiskit Documentation, 2016).

Penelitian ini berfokus untuk mengimplementasikan sirkuit kuantum algoritma Shor untuk meretas kriptografi RSA. Penelitian ini dilakukan dengan menggunakan bahasa pemrograman *python* dengan memanfaatkan Qiskit untuk merancang proses peretasan RSA dengan sirkuit kuantum algoritma Shor. Penelitian ini dilakukan untuk mengukur performa dari sisi kecepatan waktu program *user time* (Wicaksana, 2017) dari implementasi sirkuit kuantum Shor untuk meretas RSA.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan sebelumnya, rumusan masalah yang ditemukan adalah sebagai berikut.

1. Bagaimana implementasi sirkuit kuantum Shor untuk meretas kriptografi RSA menggunakan Qiskit *IBM Q Experience*?
2. Bagaimana performa dari implementasi sirkuit kuantum Shor dinilai dari segi waktu eksekusi program *user time* (Wicaksana, 2017) menggunakan Qiskit *IBM Q Experience*?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang dibawa pada penelitian ini untuk dijadikan patokan dalam penelitian kali ini. Berikut batasan masalah yang ditentukan.

1. Implementasi sirkuit kuantum Shor diterapkan menggunakan Simulator Kuantum *IBM Q Experience* dan tidak menggunakan komputer kuantum yang sebenarnya.
2. Performa implementasi sirkuit kuantum Shor diukur dari sisi waktu eksekusi program *user time* (Wicaksana, 2017).
3. Ukuran *key* RSA mengikuti jumlah *qubit* yang tersedia sesuai dengan teknologi kuantum yang digunakan.
4. Peretasan RSA dilakukan dengan tujuan untuk mendapatkan isi *plain text* hasil enkripsi RSA.
5. *Ciphertext* dan *Public-key* (N, e) diasumsikan telah diperoleh untuk simulasi peretasan RSA.

6. Bentuk *input Cipher Text* direpresentasikan dengan *ASCII* untuk proses dekripsi RSA.
7. RSA yang digunakan dibuat sendiri berdasarkan algoritma RSA dasar untuk menyesuaikan dengan jumlah *key* tersedia pada *backend* Qiskit yang mempengaruhi *range* akan enkripsi dan dekripsi yang dilakukan.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan, tujuan dari penelitian yang dilakukan adalah sebagai berikut.

1. Mengimplementasikan sirkuit kuantum Shor untuk meretas enkripsi RSA.
2. Mengetahui performa implementasi sirkuit kuantum Shor untuk peretasan kriptografi RSA dari segi waktu eksekusi program *user time* (Wicaksana, 2017).

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Memperjelas topik komputasi kuantum dan implementasi sirkuit kuantum Shor dalam peretasan kriptografi RSA.
2. Menunjukkan cara implementasi sirkuit kuantum Shor dalam peretasan enkripsi RSA.
3. Menunjukkan relasi antara jumlah *qubit* yang dibutuhkan, ukuran *key* RSA, dan *user time* (Wicaksana, 2017) yang dibutuhkan untuk meretas dan mengubah *cipher text* menjadi *plain text*.

1.6 Sistematika Penulisan

Sistematika penulisan yang dilakukan dalam laporan skripsi ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisikan latar belakang pemilihan judul skripsi "Implementasi Sirkuit Kuantum Shor Untuk Peretasan Kriptografi RSA", rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan skripsi.

BAB II LANDASAN TEORI

Bab ini berisi dasar-dasar teori yang digunakan dalam penelitian terkait dengan permasalahan yang dibahas. Teori-teori yang digunakan dalam penelitian ini antara lain *Shor's Algorithm*, *Oracle Function,* Sistem Kriptografi RSA, *Qiskit IBM Quantum Experience*.

BAB III METODOLOGI DAN PERANCANGAN PROGRAM

Bab ini berisi metodologi penelitian yang digunakan, antara lain telaah literatur, perancangan, implementasi, pengujian, serta evaluasi. Pada bagian perancangan terdapat juga fungsi aplikasi yang ada pada program implementasi, antarmuka halaman dari program yang dibuat, dan pembuatan data untuk tahap uji coba.

BAB IV IMPLEMENTASI DAN ANALISIS

Bab ini berisi hasil implementasi simulasi yang dibuat dengan sirkuit yang telah dibuat dan diikuti dengan uji coba penelusuran program menggunakan metode *white box*.

BAB V SIMPULAN DAN SARAN

Bab ini berisi simpulan dan hasil uji coba yang telah dilakukan dalam penelitian, beserta saran untuk pengembangan lebih lanjut terkait penelitian.